Authentication Intelligence

Objective

This comprehensive guide describes the actions an enterprise must complete to successfully deploy Authentication Intelligence in their system, test signals, and use the Authentication Intelligence dashboard.

Product Summary

Authentication Intelligence enables enterprises to extend the lifetime of login sessions for good users. A typical web login session usually expires in 30 minutes or an hour. Authentication Intelligence enables implicit login for eligible users, extending the session lifetime to weeks or months without reducing the security of the login session. This provides more conversions with frictionless authentication experience, a better user experience, and reduced customer support costs due to authentication friction.

Setup and Deploy Authentication Intelligence

Step 0: Kickoff

The Customer Success Team will begin conversations with the enterprise to learn about their unique user session experiences and to ensure Authentication Intelligence can help address the issue.

Step 1: Review

The Customer Success Team will engage with the enterprise to:

- clarify enterprise data collection requirements
- ensure that existing permissions don't prevent 1JS from making necessary API calls

Note: The Customer Success Team will reach out to the enterprise to inform them about any prerequisites.

Step 2: Insert 1JS

Authentication Intelligence supports easy integration options for all enterprise types. The Customer Success Team will work closely with the enterprise to recommend the right implementation approach.

Step 3: Data collection begins

Authentication Intelligence begins collecting data.

Note: The enterprise can review the data fields Authentication Intelligence is collecting by reaching out to the Customer Success Team.

Authentication Intelligence only collects information needed in order to deliver better friction reduction outcomes for enterprises. That means Authentication Intelligence may collect the following personal data:

- Username
- Data that a user inputs.
- Data provided to the user.
- Data that describes how the user, browser, and device are interacting with the website.
- Data about the user, including device identifier.

Note: Approval from the enterprise is required before this information is collected.

Step 4: Implement logic mapped to recommendation value

Extension logic should be built in advance when designing the changes in the authentication system. For example, if the server sees e7, then extend the session to 7 days. If the server sees e30, then extend the session to 30 days. (Value descriptions are located in the table below)

Planning such changes in advance ensures a smooth transition between various session lengths without repetitive code change.

Field	Description
`dc`	Device characteristics recommendation. Its values are: • `ine` - Ineligible for session extension • `e` - Recommended for session extension. This value will include additional characters to indicate session length. See the DC Values table below.
`imf`	Invisible multi-factor recommendation. Possible values are: • `ine` - Ineligible for invisible multi-factor authentication • `e` - Recommended for invisible multi-factor authentication. **Note:** If an enterprise is interested in this feature, they must contact the Customer Success Team.

`ts`	UNIX timestamp (seconds since epoch) when the Authentication Intelligence recommendation was generated. This field is used for tamper check by F5/Shape. (Enterprise can ignore this field.)
`ha`	A random ID generated for the cookie. This field is used for tamper check by F5/Shape. (Enterprise can ignore this field.)
`url`	The full URL of the request.
`rc`	Two or three digit reason code. Reason codes indicate anomalous behavior seen for the device or user, which contribute to the risk assessment. • `MUD` - Multi-user device. Sharing behavior was observed. • `SH` - Short history. The user doesn't have a long enough history with the enterprise or a strong real-time interaction. • `LOE` - Lack of evidence. No, or very little past transaction history. • `LSBH` - Lack of safe browsing history. Failed the check of safe browsing history.

DC Values

Value	**Description**	**Session Length**
`e7`	Eligible for session extension and will be given a 7 day session.	7 day
`e14`	Eligible for session extension and will be given a 14 day session.	14 day
`e30`	Eligible for session extension and will be given a 30 day session.	30 day
`e60`	Eligible for session extension and will be given a 60 day session.	60 day
`e90`	Eligible for session extension and will be given a 90 day session.	90 day
`ec`	Eligible for session extension and will be given a session length set by the enterprise. This group usually serves as	Enterprise session length without Authentication Intelligence

	the control group for initial A/B testing.	**Note:** The session length the enterprise has configured for their regular end user

Note: The session length the enterprise has configured for their regular end user.

Step 5: Authentication Intelligence sends recommendations in cookie

After 1JS has collected data for 30 days, Authentication Intelligence will send the enterprise system recommendations in an encrypted cookie named `_imp_apg_r_`.

Step 6: Enterprise decrypts cookie

Note: If the enterprise is unable to decrypt a cookie, then review alternate options with the Customer Success Team.

Recommendations are sent in the `_imp_apg_r_` cookie (JSON format) within the “c” dictionary. Below is an example cookie value (after URL decoding).

```
_imp_apg_r_: {"c":"OUhHYVd4TW5nNXM2SUpmYw==ZZzzNnGYV1hlPlxGjYayN6ba..."}
```

Cookie encryption and decryption logic

The Customer Success Team will share the decryption key with the enterprise.

Crypto algorithm

- Algorithm: AES/GCM/NoPadding (AES-CBC if use BigIP deployment)
- Key Size:128 bits
- Initialization Vector (IV): 16 bytes
- Encoding: Base64URL, i.e. URL safe base64 encoding.

```
Output = Base64URL(IV) + Base64URL(CT + TAG)
```

Note: The “+” means concatenation in the above expression.

```
import base64
from cryptography.hazmat.backends
import default_backend
from cryptography.hazmat.primitives.ciphers import(
Cipher, algorithms, modes
)

def aes_decrypt(key, ciphertext, iv, tag):
      #Construct an AES - GCM Cipher object with the given key and a
      # randomly generated IV.
      decryptor = Cipher(
            algorithms.AES(key),
            modes.GCM(iv, tag),
            backend = default_backend()
      ).decryptor()

      # Encrypt the plaintext and get the associated ciphertext.
      # GCM does not require padding.
      plaintext = decryptor.update(ciphertext) + decryptor.finalize()
      return plaintext

def pegasus_aes_decrypt(key, cipher):
      # base64 input is of type 'byte'
      if type(cipher) != bytes:
            cipher = cipher.encode()
      iv = base64.urlsafe_b64decode(cipher[: 24])
      cipher_and_tag = base64.urlsafe_b64decode(cipher[24: ])
      cipher_text = cipher_and_tag[: -16]
      tag = cipher_and_tag[-16: ]# call aes_decrypt to decrypt

      plaintext = aes_decrypt(key, cipher_text, iv, tag)
      print('plain text is %s' % plaintext)
      return plaintext

      # Simple test
      key = b '0123456789abcdef'
      cipher = 'dzZCQUVIaTBPa2FZYkdEQQ==_mzQrFAp-yiP_-pY9rH3aokwPotI'
      pegasus_aes_decrypt(key, cipher)
```

Encrypted data format

The encryption uses a randomly generated Initialization Vector (IV), which is 128 bits. The output of the AES encryption algorithm is cipher text (CT) and the fixed-length tag of exactly 16 bytes (TAG). So the 3 parts, IV, CT and TAG, go into the final output.

Step 7: Enterprise enforces action

Based on value recommendations, extend the session length or modify authentication behavior accordingly. (Please refer to Step 4: Implement logic mapped to recommendation value.)

Troubleshoot and Escalation Process

The enterprise should reach out to the Customer Success Team.

Signal Descriptions

Personal infrastructure (device)

Authentication Intelligence uses a concept called Personal Infrastructure which consists of network signals, hardware signals, and software signals, all of which are assessed on a cross-enterprise basis. The Authentication Intelligence documentation uses the terms personal infrastructure and device interchangeably for convenience.

Personal Infrastructure (or device) has three components. Examples of data elements in each of these components include:

- Network signals: IP address and reputation, ASN, geolocation
- Hardware signals: GPU, number of cores, screen size
- Software signals: browser attributes, plugin list, font list

F5 assumes that these and other signals are actively spoofed by attackers. However, Authentication Intelligence never relies on these signals alone to deem a user eligible for session extension. Rather, it uses these signals in conjunction with many others to make its recommendations.

The combination of these signals allows F5 to make strong assertions about legitimate users returning to a given website while operating the same device they had previously used to log in.

Session extension: data used to make recommendation

Authentication Intelligence provides enterprises with a signal as to whether the visitor to a given website should be given an extended session (e.g. 30 days) or a default session (typically 30 minutes). This recommendation comes from three categories of information applied against a given device: history, uniqueness, and integrity. Authentication Intelligence identifies returning legitimate users by answering the following questions about a user and the device they are operating:

- **History:** Did this user, from this device, successfully log into the website previously?
- **Uniqueness:** Is this device operated by a single human user?
- **Integrity:** Does F5 believe this device and account are safe?

If the answers to all of the above are yes, then Authentication Intelligence considers a user for an extended session. The actual model behind session extension is much more complex than this. For example, F5 has model-derived parameters for how much history is required, and takes into account whether the user operates multiple devices. But this provides a high-level summary of the core elements of the system.

Cross-enterprise attestations

As a further check, Authentication Intelligence asks all of the questions above across multiple enterprises that use F5. This group includes approximately 40% of the B2C brands in the Fortune 500, so F5 evaluates history, uniqueness, and integrity across many different types of websites. Importantly, some websites are low-frequency/high-value, such as telco sites, and others are high-frequency/low-value, like quick-serve restaurant sites. A user who has only logged into enterprise A's website once in the prior year might have logged into other F5-protected websites many times in the same time period. Conversely, a device which supports a single user on enterprise A may support multiple users on some other website (this would constitute a “no” to question #2).

At no point does F5 ever share data across enterprises. Affirming or contravening data points simply change the final recommendation Authentication Intelligence makes for a given transaction.

At a very simple level, if any of the questions listed above are untrue on enterprise A’s website, or any other website that uses F5, then Authentication Intelligence will not recommend an extended session. In practice, F5’s model accounts for significant complexity, such as shared computers (hotels, libraries), family environments with multiple users, occasional sharing of a device, and other scenarios. F5 errs strongly on the side of conservatism in these and other scenarios.

Sample data elements of history, uniqueness, and integrity

The three categories described above, which allow Authentication Intelligence to determine when to extend sessions, have many components. Some of the components include:

History
Because other F5 products are already in-line to help mitigate bots and automation, Authentication Intelligence has deterministic information about historical login activity. Authentication Intelligence constructs a graph of all successful account logins, and all devices performing such logins, and uses this to identify legitimate returning users.

Uniqueness
F5 is able to determine whether, for a single device, more than a single user has ever successfully logged into a given website. Further, F5 can determine whether more than one unique user has logged into other websites protected by F5. If, within a given measurement window, F5 only sees a single unique user logging into each website protected by F5, then F5 deems that device to be operated by a single human being.

Integrity
Authentication Intelligence evaluates integrity across multiple dimensions. Before considering a session extension, Authentication Intelligence evaluates questions such as:

- Has a user with this device performed successful transactions on one or more F5-protected websites?
- Has this user's account been accessed in abnormal ways (for example, by a large number of devices)?
- Does either part of the credential appear in F5's spilled credential service (requires Blackfish to be enabled)?
- Do interrogated device characteristics match published characteristics?

Signal Testing

Enterprises should adjust their authentication experience based on F5's signal. F5 provides two cookies configured to generate an eligible and ineligible status. Both cookies enable unit and integration testing.

Test Cookies

The Authentication Intelligence testing cookies are described below:

Test Cookie	Value Returned with dc	What does it mean?
A---64psAQAA-testlabel-unknown-aoho4L6JYmf7pR8La9UHUK4ovifs024879TWaf4	ine	Ineligible for session extension
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987	e	Recommended for session extension.
A---64psAQAA-testlabel-shared-mxoZeyD898TS0ioiM1oAQeF2GPcD5UwJ-m0dQa	ine	Ineligible for session extension
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987-0	ec	Eligible for session extension and will be given a session length set by the enterprise. This group is usually served as the control group for initial A/B testing.
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987-7	e7	Eligible for session extension and will be

		given a 7 day session.
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987-14	e14	Eligible for session extension and will be given a 14 day session
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987-30	e30	Eligible for session extension and will be given a 30 day session.
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987-60	e60	Eligible for session extension and will be given a 60 day session.
A---64psAQAA-testlabel-private-9gt798eqWq2RQdagaXag234GbVclPh1Aa0987-90	e90	Eligible for session extension and will be given a 90 day session.

After F5 enables the signal

1. Open **Inspect**.
2. Go to www.customer.com .
3. Go to any page where the Authentication Intelligence JavaScript has been embedded.
4. Click **Application** > **Cookies**.
5. Select the www.customer.com domain.
6. To test on APG cookie injection, find a cookie with the key = '_imp_apg_r' .

After the enterprise implements signal consumption to extend session length

1. Open **Inspect**.
2. Go to www.customer.com .
3. Go to any page where the Authentication Intelligence JavaScript has been embedded.
4. Click **Application** > **Cookies**.
5. Select the www.customer.com domain.
6. To test on APG cookie injection, find a cookie with the key = '_imp_apg_r' .
7. To further test on decryption & authentication functionality using APG cookie
    a. Delete the APG cookie current value
    b. Fill in with the APG cookie value provided by F5. Choose the "encrypted + encoded" version.
8. Refresh the page.
    a. With sample APG cookie signaling eligible for session extension, users should be logged in.
    b. With sample APG cookie signaling ineligible for session extension, users stay unauthenticated.

More actions may be required depending on the re-authentication design at the enterprise's backend.

Dashboard

Overview

This section provides information about accessing and using the Authentication Intelligence Interface & Dashboard, and a brief summary of the visual components.

Access

For access and credentials to the Authentication Intelligence Interface & Dashboard, please contact your technical account manager.

Introduction

The Authentication Intelligence Interface & Dashboard allows customers to view data visualizations which illustrate how session length extensions help rescue customers and create business value.

Views

Authentication Intelligence supports two views: “Before extending sessions” and “After extending sessions”.

- “Before extending session” - This view is available before extensions are enabled. The purpose of this view is to show the value and potential success of recusing customers when sessions are extended.
- “After extending sessions” - This view is only available after extensions are enabled. The purpose of this view is to illustrate the real-world impact and benefit that extending sessions has made to your organization.

Note: Dashboards are built based on F5’s best understanding of enterprises’ deployment and website behavior. Analytical models may require updates if traffic routing or website login experience changes.

Interpreting Data

The Authentication Intelligence interface features three tabs: Conversions & Revenue, Dashboard, and Rescue Customers.

- **Conversions & Revenue:** Shows real or predicted changes in conversions and revenue over time when session length is modified.
- **Dashboard:** Dive into user login and conversion behavior when enjoying longer sessions.
- **Rescue Customers:** Shows user login friction and how would increase session length help frustrated users.

Note: Data will not be present in the Authentication Intelligence interface until 1JS is injected into your organization's web flows and has a compliant history for at least 30 days.

You can control the range of data displayed by using the date range picker and the Display Interval menu (when shown).

- Select the date range of interest, and pick a display interval upon which data aggregation will execute.

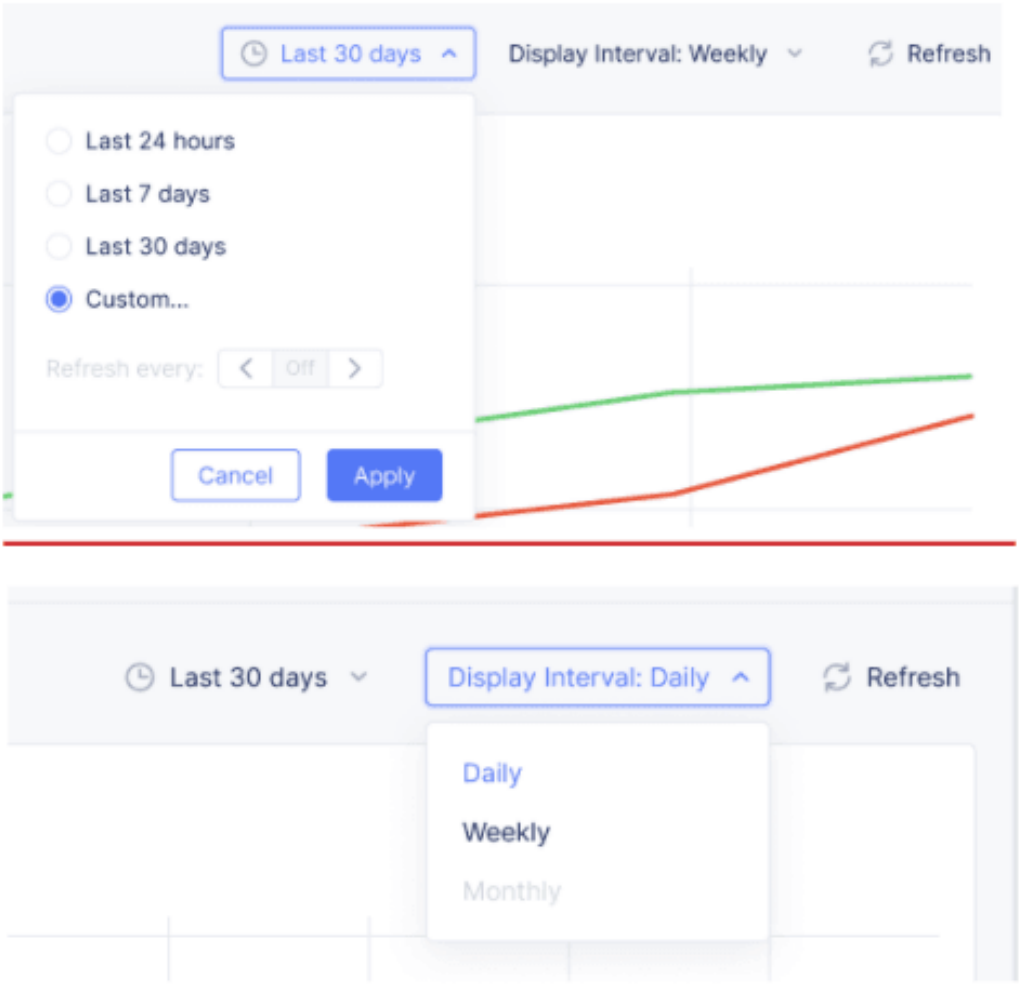

Figure: Select data ranges

Before extending sessions

1JS is not present
If your organization hasn't extended sessions and hasn't injected 1JS into its web flow, the Authentication Intelligence tabs will be empty. You might see placeholder data like in the screenshot below:

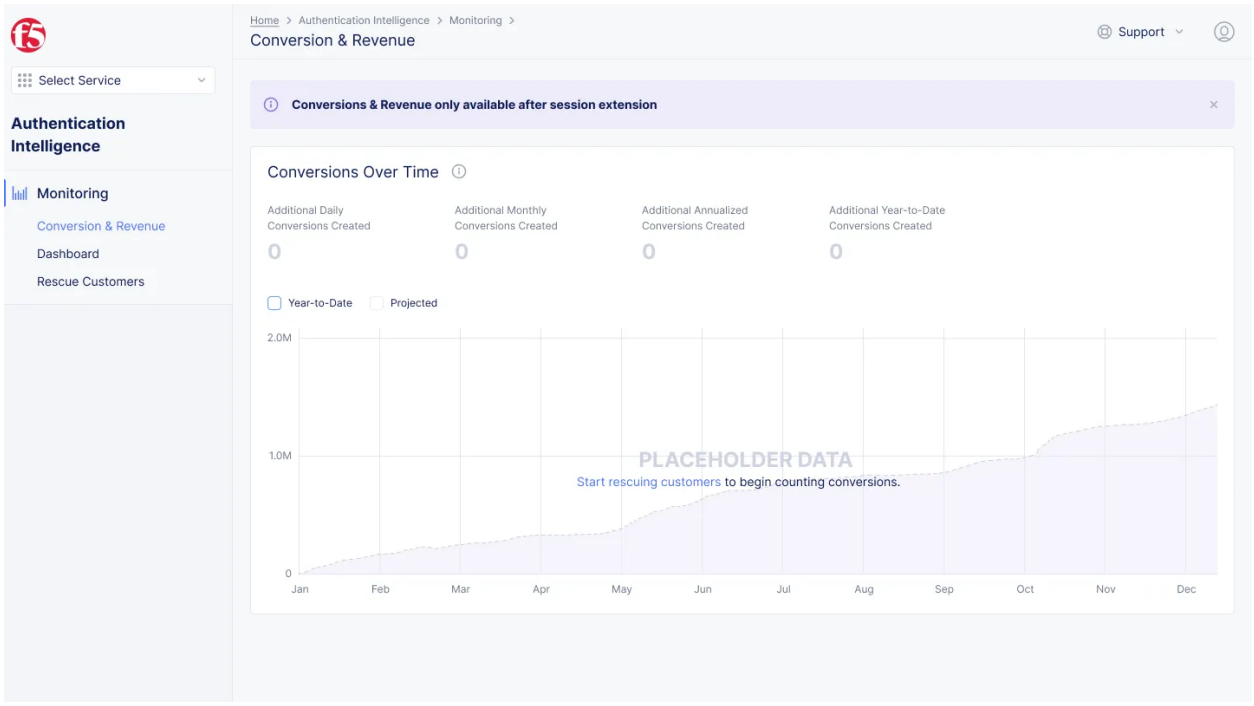

Figure: Empty Tab

1JS is present

If your organization has injected 1JS into its web flow, but not extended sessions yet, then the Rescue Customers tab will be populated with some data. (The Conversions & Revenue and Dashboard tabs will remain empty until session length is extended.)

- “Users Who Experienced Login Friction”: Includes your organization's customer login data. The component will demonstrate the percentage of customers who experienced login friction including those customers who were never able to log in.
- “Percentage of Users That Can Be Spared Friction”: Percentages of users that can be rescued from login pain - sorted by friction type.
- “Volume of Users That Can Be Spared Friction”: Volumes (raw numbers) of users that can be rescued from login pain - sorted by friction type.
- “Daily Login Friction”: Daily report of known good users experiencing unnecessary pain from login challenges.

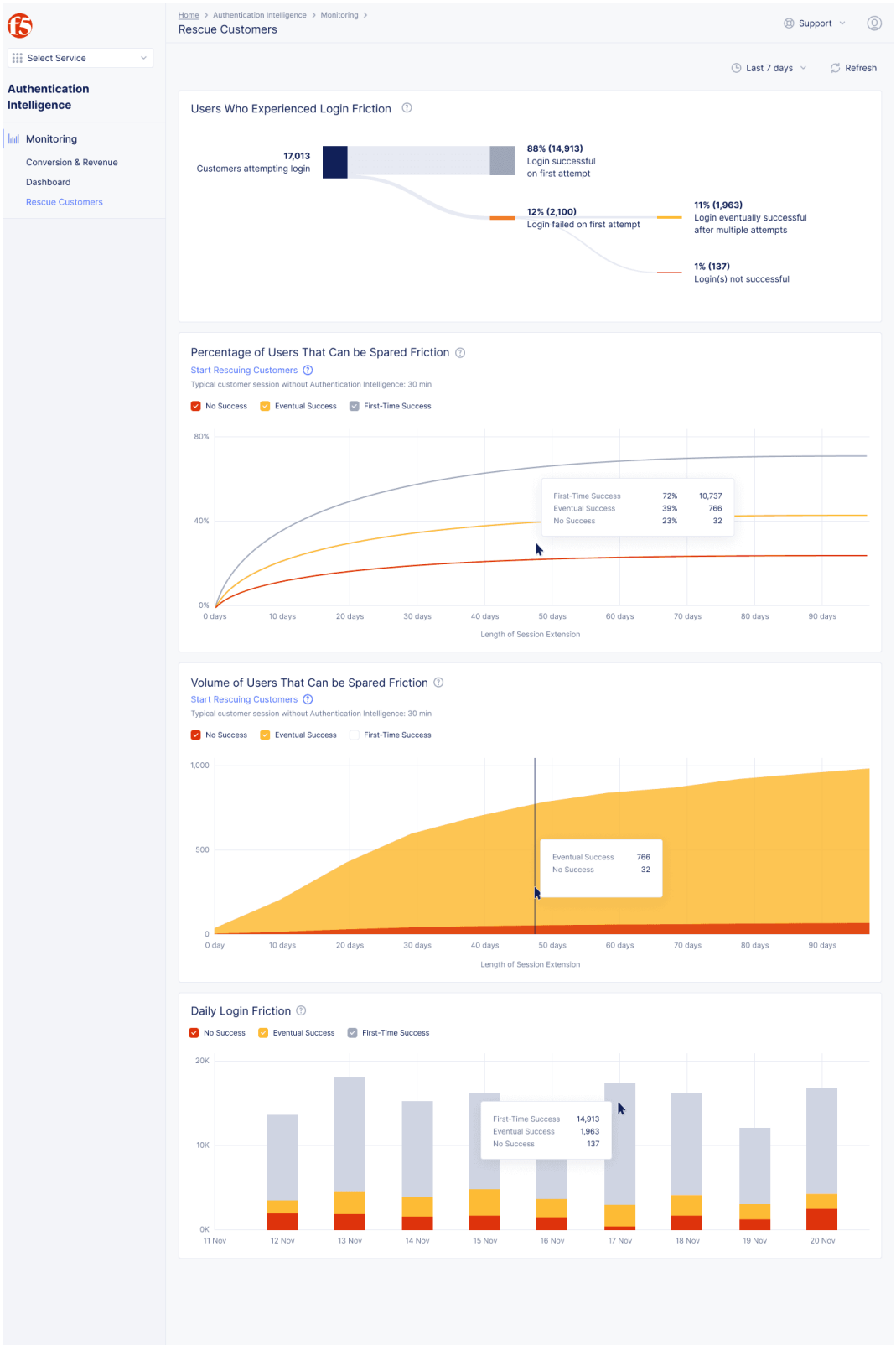

Figure: 1JS is present

After extending sessions

Conversions & Revenue Tab

After sessions are extended, the following components are filled with data:

- “Conversions Over Time”: The amount of additional conversions over a certain period of time that resulted from extending session length.
- “Revenue Over Time”: The amount of additional revenue earned over a certain period of time that resulted from extending session length. "Revenue Over Time" is equal to "Conversions Over Time" multiplied by average transaction amount input by dashboard users.

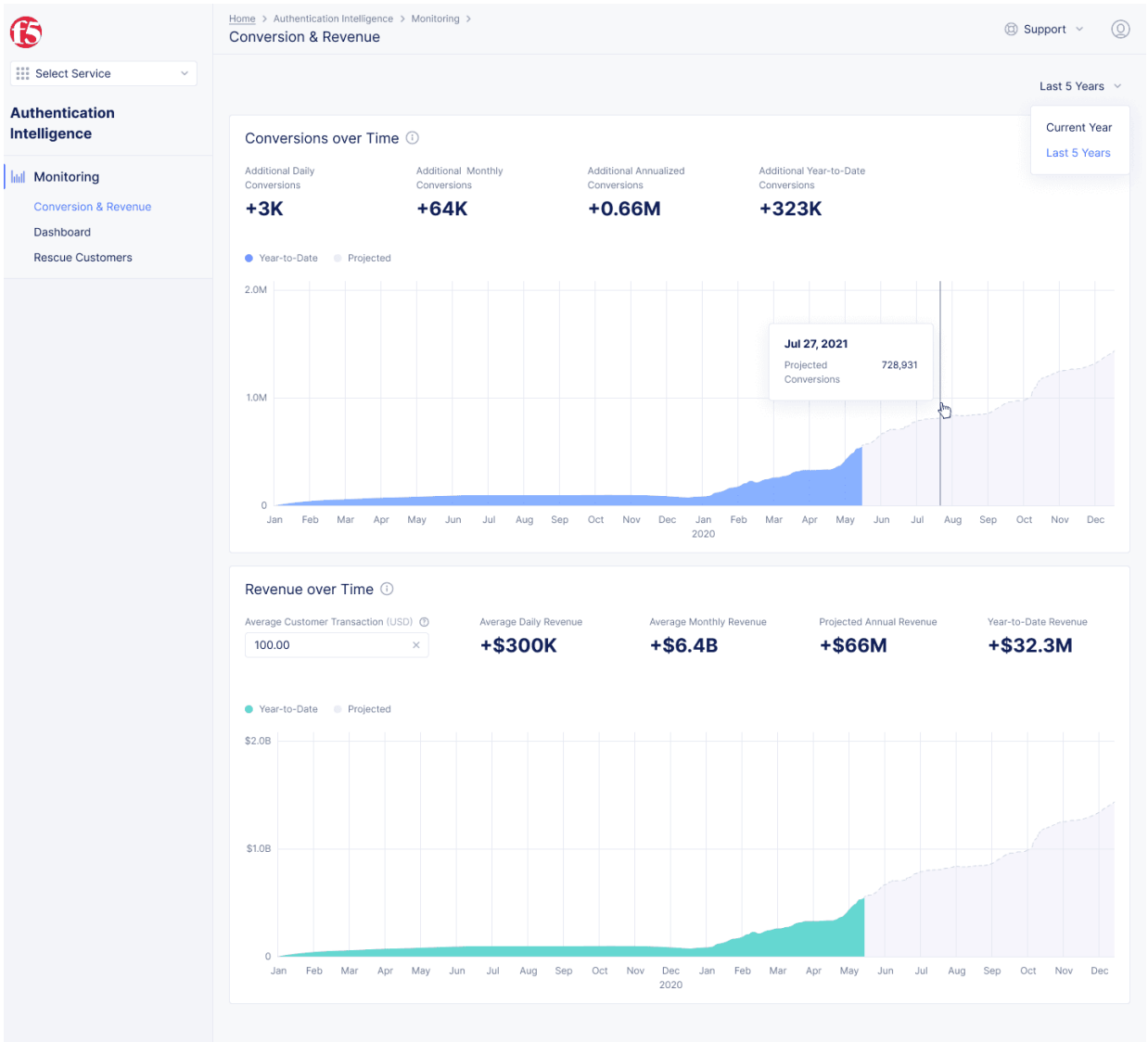

Figure: Conversions & Revenue Tab

Dashboard Tab

- “Conversion Lift Over Time”: Compares real-life conversion rates between your users who benefited from session extension and a control group.
- “Users Enjoying Silent Reauthentication”: The amount of users who benefitted from session extension.
- “User Channels”: Users who benefited from session extension by device type (Desktop Web or Mobile Web).

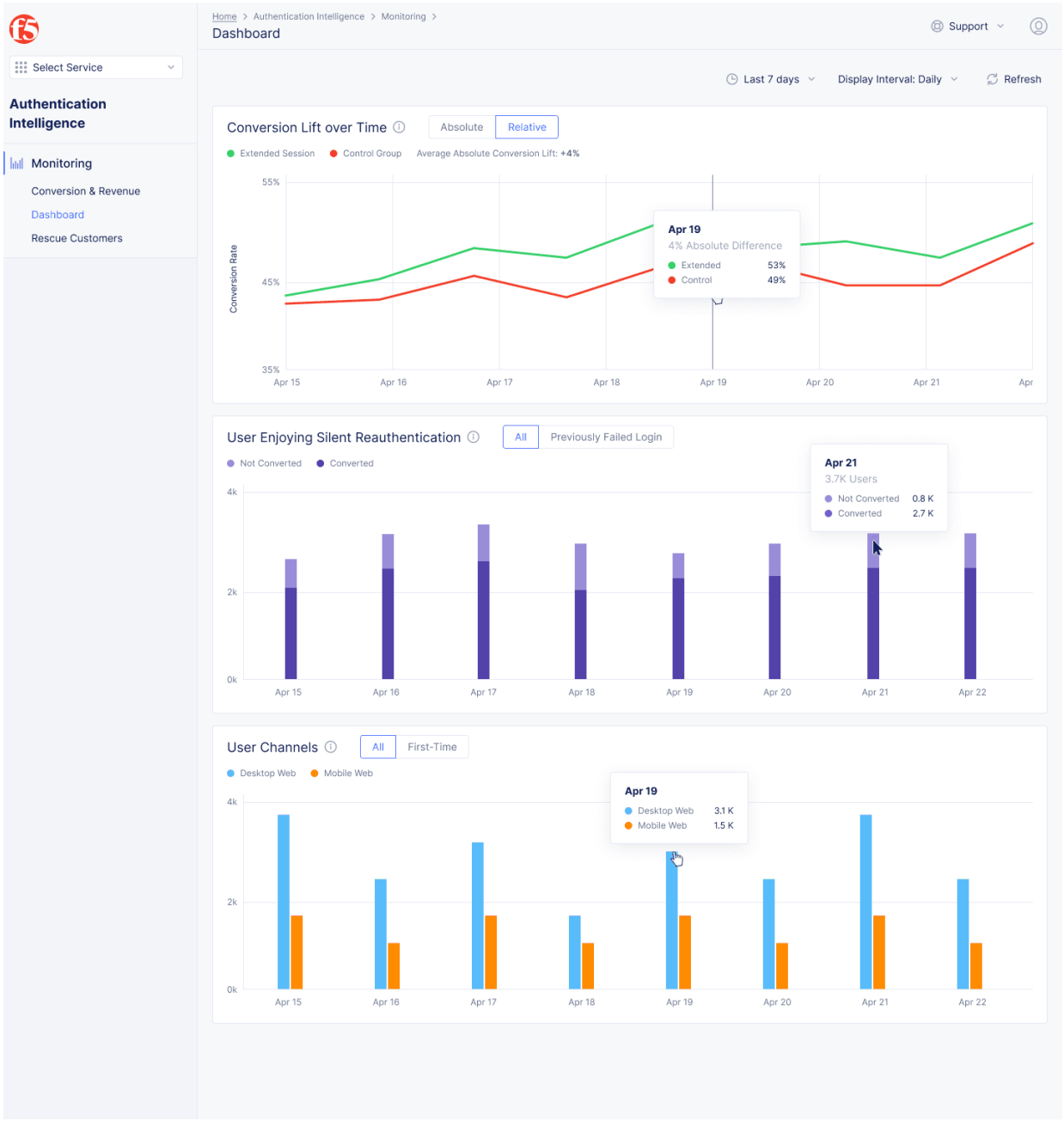

Figure: Dashboard Tab

Rescue Customers Tab

- “Rescue Customers”: Summarizes the current rate of users who abandoned logins and experienced friction, and the potential benefit your organization can earn if session lengths are extended over a longer period. The component makes it easy to increase session length and get extra help via hyperlinks in the interface.

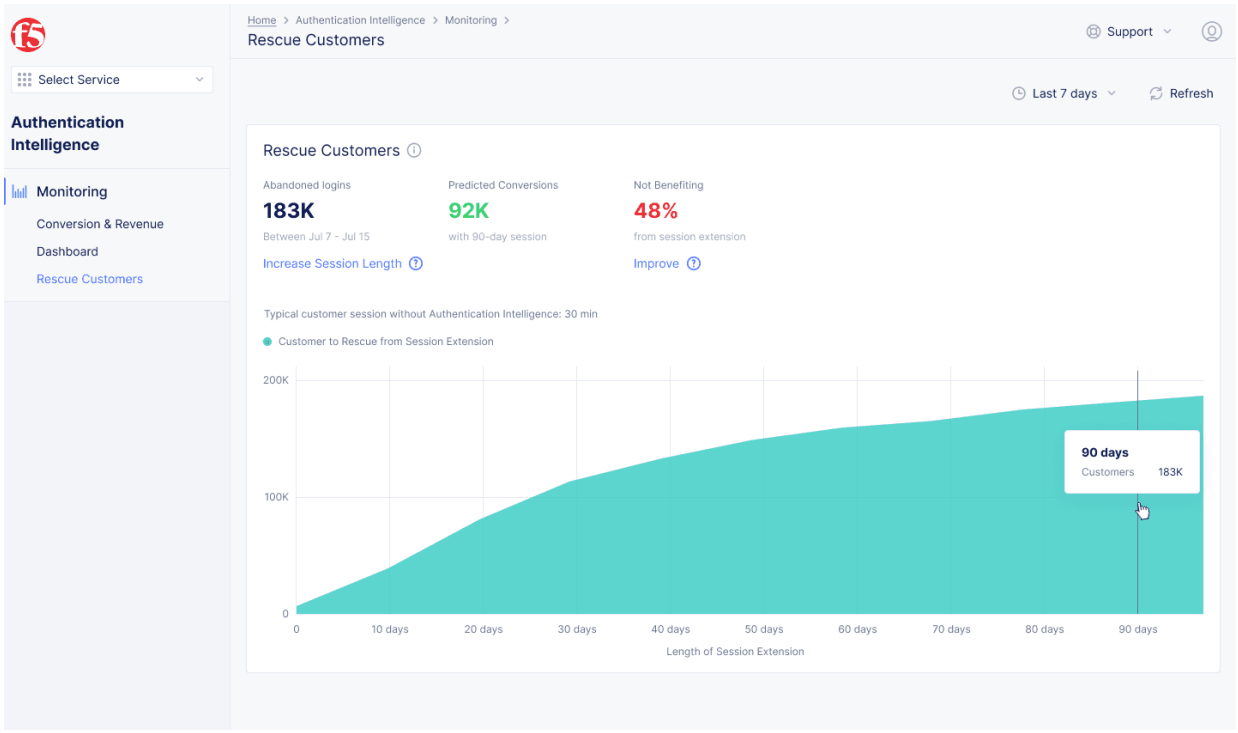

Figure: Rescue Customers Tab